EXHIBIT 17

US009198117B2

(12) **United States Patent**
Raleigh

(10) **Patent No.: US 9,198,117 B2**
(45) **Date of Patent: Nov. 24, 2015**

(54) **NETWORK SYSTEM WITH COMMON SECURE WIRELESS MESSAGE SERVICE SERVING MULTIPLE APPLICATIONS ON MULTIPLE WIRELESS DEVICES**

(71) Applicant: **Headwater Partners I LLC**, Redwood City, CA (US)

(72) Inventor: **Gregory G. Raleigh**, Woodside, CA (US)

(73) Assignee: **Headwater Partners I LLC**, Redwood City, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **14/667,516**

(22) Filed: **Mar. 24, 2015**

(65) **Prior Publication Data**

US 2015/0200882 A1 Jul. 16, 2015

Related U.S. Application Data

(63) Continuation of application No. 14/263,604, filed on Apr. 28, 2014, now Pat. No. 9,037,127, which is a continuation of application No. 12/380,780, filed on Mar. 2, 2009, now Pat. No. 8,839,388.

(Continued)

(51) **Int. Cl.**
G06F 15/16 (2006.01)
H04L 9/32 (2006.01)
(Continued)

(52) **U.S. Cl.**
CPC ***H04W 48/14*** (2013.01); ***G06F 15/177*** (2013.01); ***G06Q 10/06375*** (2013.01);
(Continued)

(58) **Field of Classification Search**
USPC 709/203, 204, 206, 207, 217, 219, 223; 713/168–170; 705/28, 30; 455/405, 455/406, 411, 414.1
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,131,020 A 7/1992 Liebesny et al.
5,283,904 A 2/1994 Carson et al.
(Continued)

FOREIGN PATENT DOCUMENTS

CA 2688553 A1 12/2008
CN 1310401 A 2/2000
(Continued)

OTHER PUBLICATIONS

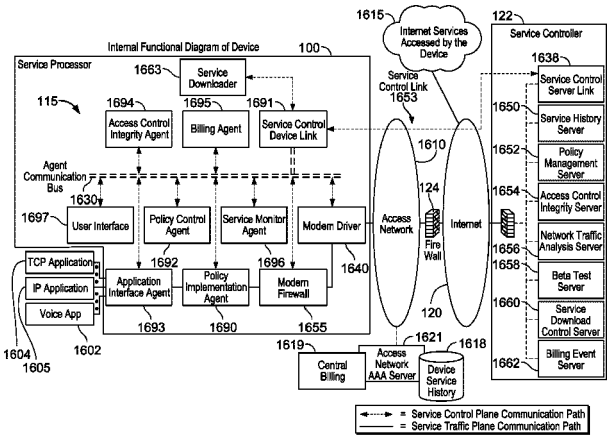
VerizonWireless.com news, "Verizon Wireless Adds to Portfolio of Cosumer-Friendly Tools With Introduction of Usage Controls, Usage Controls and Chaperone 2.0 Offer Parents Full Family Security Solution," Aug. 18, 2008.
(Continued)

Primary Examiner — Andrew Joseph Rudy
(74) *Attorney, Agent, or Firm* — James E. Harris

(57) **ABSTRACT**

Each of several mobile end-user devices contains a device messaging agent that securely communicates with a network message server over a wireless network. The network message server delivers messages to the device messaging agent on behalf of a plurality of network application servers. Each network application server supplies the network message server with application data and an indication of a device and an application on the device to which the application data should be delivered. The network message server securely passes the data and an application identifier to the device messaging agent on the appropriate mobile end-user device. The device messaging agent maps the application identifier to a software process corresponding to the application, and a secure interprocess communication service delivers the application data to that software process.

18 Claims, 106 Drawing Sheets



surveys over the intermediate networking device control channel. In some embodiments, the service processor **115** has a VPN connection to a network base station hand off controller to assist in handoff to and from the WWAN network and/or has the capability to instruct the end point device and the base station handoff controller. In some embodiment, whenever an end point device authenticated for femto cell access is within range of the femto cell, the service provider desires to set up a service processor **115** profile to get the end point device to connect to the femto cell even if it has a strong signal with one or more WWAN base stations so that the WWAN traffic may be offloaded. In some embodiments, the service processor **115** can form a secure control plane link with network AAA functions to manage authorization and admission of end point devices the femto cell has not yet admitted, or the network policies can require re-authorization every time a end point device attempts access. Once an end point device is connected to the femto cell intermediate networking device, the verifiable traffic monitoring, control and billing functions described herein can be applied to various application embodiments. For example, the intermediate networking device service policy verification techniques disclosed herein, as similarly described with respect to various device embodiments, can similarly be applied to the femto cell intermediate networking device embodiments.

In some embodiments, the service provider desires to keep the number of end point devices or users that access an intermediate networking device below a certain count specified in the service processor **115** profile. In some embodiments, this is accomplished by controlling the number of IP addresses allowed onto the intermediate networking device local area side connection. In some embodiments, this is facilitated by observing the end point device identification parameters available in the end point device traffic. In some embodiments, this is facilitated by observing the traffic patterns to determine the likely number of devices connecting to the network. For example, traffic demand patterns can be examined to determine how many users are likely to be demanding access at one time. Although the foregoing embodiments have been described in some detail for purposes of clarity of understanding, the invention is not limited to the details provided. There are many alternative ways of implementing the invention. The disclosed embodiments are illustrative and not restrictive.

What is claimed is:

1. A network system comprising:

a plurality of device messaging agents, each executable on a respective one of a plurality of mobile end-user devices configured to exchange Internet data via a data connection to a wireless network; and

a network message server

supporting a plurality of secure Internet data connections, each secure Internet data connection between the network message server and a respective one of the mobile end-user devices via a device data connection to a wireless network,

the network message server configured to receive, from each of a plurality of network application servers, multiple requests to transmit application data, each such request indicating a corresponding one of the mobile end-user devices and one of a plurality of applications,

the network message server to generate corresponding Internet data messages based on the requests, each such message containing at least one application identifier for an indicated application and application data corresponding to one of the requests, and

the network message server to transmit each of the generated Internet data messages to the device messaging agent located on the device indicated in the corresponding request, using the corresponding secure Internet data connection for the device indicated in the corresponding request;

each device messaging agent, when executing,

to receive the Internet data messages from the secure Internet data connection corresponding to the device executing the device messaging agent, and

to, for each received message, map the application identifier in the message to a software process corresponding to the application identifier, and forward the application data in the message to the software process via a secure interprocess communication service.

2. The network system of claim **1**, the network message server further to collect and buffer multiple requests to transmit application data to a particular one of the devices.

3. The network system of claim **1**, wherein the plurality of applications include a first application that receives the application data in a first format, and a second application that receives the application data in a second format different than the first format.

4. The network system of claim **1**, the network message server further to encrypt the secure Internet data messages, the device messaging agents further to decrypt each received message to obtain the corresponding application identifier and application data.

5. The network system of claim **4**, wherein the secure Internet data messages are transported to the device messaging agent on each device using one or more of encryption on a transport services stack, IP (Internet Protocol) layer encryption, and tunneling.

6. The network system of claim **1**, wherein the device messaging agent executes in a secure execution environment on at least one of the devices, and at least one of the applications executes outside of the secure execution environment on that device.

7. The network system of claim **1**, wherein:

at least a subset of the device messaging agents, when respectively executing on their respective devices, are each further to

receive, from each of multiple applications executing on the corresponding device, at least one corresponding request to transmit application data, each such request indicating a corresponding one of the network application servers,

generate corresponding upload Internet data messages based on the requests, each such message containing at least one server identifier for an indicated application server and application data corresponding to one of the requests, and

transmit each of the generated upload Internet data messages to the network message server, using the corresponding secure Internet data connection for the device; and

the network message server is further to

receive the upload Internet data messages over the respective secure Internet data connections, and

for each received upload Internet data message, map the server identifier in that message to a corresponding one of the network application servers, and transmit the application data from that message to the corresponding network application server, together with an indication of the device from which that message was received.